JOURNAL OF NUMBER THEORY 5, 379–384 (1973)

The Trace-Form of an Algebraic Number Field

DONALD MAURER

Department of Mathematics, Tufts University, Medford, Massachusetts 02155

PRESENTED AT THE QUADRATIC FORMS CONFERENCE, BATON ROUGE, LOUISIANA, MARCH 27–30, 1972, AND DEDICATED TO THE MEMORY OF LOUIS JOEL MORDELL

Let F be the rational field or a p-adic field, and let K an algebraic number field over F. If $\omega_1, \ldots, \omega_n$ is an integral basis for the ring $\mathfrak{O}_K$ of integers in K, then the quadratic form Q whose matrix is $(\mathrm{trace}_{K|F}(\omega_i\omega_j))$ has integral coefficients, and is called an integral trace-form. Q is determined by K up to integral equivalence. The purpose of this paper is to show that the genus of Q determines the ramification of primes in K.

I. Let F denote the rational field $\mathbf{Q}$ or a p-adic field $\mathbf{Q}_p$, and let K be a finite algebraic extension field of F. We shall use d_K to denote the field discriminant of K over F, and $T_{K|F} : K \to F$ will denote the usual trace-map. We regard K as a regular quadratic space over F with respect to the bilinear form $B(x, y) = T_{K|F}(xy)$, and let $Q(x) = B(x, x)$ be the associated quadratic form. Then it is evident that the ring $\mathfrak{O}_K$ of integers in K is an integral lattice (i.e., $B(\mathfrak{O}_K, \mathfrak{O}_K) \subseteq \mathfrak{O}_F$), and if $\omega_1, \ldots, \omega_n$ is an $\mathfrak{O}_F$-basis for $\mathfrak{O}_K$, then $\det(B(\omega_i, \omega_j)) = d_K$. Hence the quadratic form Q whose matrix is $(B(\omega_i, \omega_j))$ is integral and is determined up to integral equivalence. Such a form will be called an *integral trace-form*.

The rational invariants of K, as a quadratic space, are: (i) its dimension $n = [K : F]$; (ii) $d_K/\dot{F}^2$ (i.e., the field discriminant modulo the nonzero squares); and (iii) the Hasse-invariants S_pK for each prime p (including $p = \infty$) and, if $F = \mathbf{Q}$, the positive index $\mathrm{ind}^+ Q$. In 1968 O. Taussky [3] proved that if $F = \mathbf{Q}$, and r_1 is the number of real conjugate fields and $2r_2$ the number of complex conjugate fields, then $\mathrm{ind}^+ Q = r_1 + r_2$. Other than this, little seems to be known about the connection between the trace-form and its associated field. The purpose of this paper is to determine a complete set of invariants for the genus of Q. We prove the following theorem.

THEOREM. *Let K and K' be finite algebraic extension fields of F*

(normal if $F = \mathbf{Q}$) with odd discriminant. Also suppose that the integral trace-form Q is primitive. Then gen Q = gen Q' if and only if

(i) *Q and Q' have the same rational invariants, with $d_K = d_{K'}$, and*

(ii) *if $(p) = \mathfrak{P}_1^{e(p)} \cdots \mathfrak{P}_g^{e(p)}$ is the factorization of p in K, then $e(p) = e'(p)$ for all finite primes p.*

2. Reduction to the Local Case

We do not yet assume that $K \mid F$ is normal; hence if p is a prime let

$$(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

be its factorization in K, and let f_i be the degree of $\mathfrak{P}_i$. If we set $V = K \otimes_{\mathbf{Q}} \mathbf{Q}_p$, then the bilinear form B can be "lifted" to V by defining

$$B_V(\omega_i \otimes 1, \omega_j \otimes 1) = B(\omega_i, \omega_j)$$

and it is easy to verify that $B_V(x, y) = T_{V|\mathbf{Q}_p}(xy)$. Hence V is a regular quadratic space over $\mathbf{Q}_p$ of dimension n. Moreover, we have a direct product decomposition.

$$V = \coprod K_i,$$

where K_i is a local extension of $\mathbf{Q}_p$, and $(p) = \mathfrak{P}_i^{e_i}$ in K_i. Since the K_i are the invariant subspaces of the regular representation, we further obtain an orthogonal splitting

$$V = \perp K_i.$$

The "p-ification" of $\mathfrak{O}_K$ in V is defined as

$$(\mathfrak{O}_K)_p = \coprod_i \mathfrak{O}_p(\omega_i \otimes 1);$$

($\mathfrak{O}_p$ will denote the integers in $\mathbf{Q}_p$) and clearly $(\mathfrak{O}_K)_p \subseteq \perp \mathfrak{O}_{K_i}$. Since $d_K = \prod d_{K_i}$, we have equality. Hence there is a basis for $(\mathfrak{O}_K)_p$ over $\mathfrak{O}_p$ relative to which the matrix of the form Q_V is

$$\begin{bmatrix} D_1 & & 0 \\ & \ddots & \\ 0 & & D_g \end{bmatrix}$$

where D_i is the matrix of an integral trace-form on K_i.

Lemma 1. *The form Q is primitive if and only if for each prime p, which divides d_K, there is at least one prime ideal divisor $\mathfrak{P}$ of p, in K, which is tamely ramified.*

Proof. By the preceding remarks, we can assume $F = \mathbf{Q}_p$, and so $(p) = \mathfrak{P}^e$. Let — denote the canonical map of $\mathfrak{O}_K$ into its residue class field. Then for $x \in \mathfrak{O}_K$, we have

$$\overline{T_{K|F}(x)} = eT_{\bar{\mathfrak{O}}_K|\bar{\mathfrak{O}}_F}(\bar{x}).$$

Hence p divides e if and only if

$$T_{K|F}(x) \equiv 0 (\mathrm{mod}\, p) \qquad \text{for all} \quad x \in \mathfrak{O}_K,$$

for the trace-map on finite fields is surjective. And it is evident that the scale of $\mathfrak{O}_K$ is

$$\mathfrak{s}\mathfrak{O}_K = T_{K|F}(\mathfrak{O}_K).$$

Let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathfrak{O}_K$, and let $\mathfrak{a}$ be an integral ideal. If $\alpha_1, \ldots, \alpha_n$ is an integral basis for $\mathfrak{a}$, the $\mathfrak{O}_F$-integral matrix A is called an *ideal matrix* for $\mathfrak{a}$ if

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = A \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}.$$

It is clear that every ideal matrix of $\mathfrak{a}$ has the form UAV for some $\mathfrak{O}_F$-integral unimodular matrices U and V. Assume that

$$\mathfrak{a} = \mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_g^{r_g},$$

and that $r_1 = e_i k_i + h_i$ $(0 \leqslant h_i < e_i)$. Then it is known (e.g., [1] or [4] that $\mathfrak{a}$ has an ideal matrix of the form

$$\begin{bmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_g \end{bmatrix}, \qquad \text{with} \qquad B_i = \begin{bmatrix} p^{k_i+1}A & 0 \\ 0 & p^{k_i}B \end{bmatrix},$$

where A and B are diagonal and unimodular. In particular, if $F = \mathbf{Q}_p$, then $g = 1$. We shall use this to prove

LEMMA 2. *Let $F = \mathbf{Q}_p$. Suppose D is the matrix of an integral trace-form Q and $\mathfrak{s}\mathfrak{O}_K = p^\nu$. Then there exist unimodular $\mathfrak{O}_F$-matrices U and V such that*

$$UDV = \begin{bmatrix} p^\nu M & 0 \\ 0 & p^{\nu+1}N \end{bmatrix},$$

where M and N are diagonal and unimodular.

Proof. Let $\omega_1,\ldots,\omega_n$ be an integral basis for $\mathfrak{O}_K$, and $\omega_1^*,\ldots,\omega_n^*$ the dual basis (i.e., $T_{K|F}(\omega_i\omega_j^*) = \delta_{ij}$), then

$$\begin{bmatrix} \omega_1^* \\ \vdots \\ \omega_n^* \end{bmatrix} = D^{-1} \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix},$$

for consider the linear transformation of $K \to K$ defined by $\omega_i^* \to \omega_i$ $(i = 1, 2,\ldots, n)$. Let (s_{ij}) be its matrix relative to the dual basis; then

$$\omega_i\omega_j = s_{i1}\omega_1^*\omega_j + \cdots + s_{in}\omega_n^*\omega_j$$

and so $s_{ij} = T_{K|F}(\omega_i\omega_j)$. Since the complimentary module $\mathfrak{O}_K^*$ is a fractional ideal, $d_K\mathfrak{O}_K^*$ is an *integral* ideal which has d_KD^{-1} as an ideal matrix. We then set $d_K\mathfrak{O}_K^* = \mathfrak{P}^r$, and apply our previous remarks to find unimodular matrices U_1 and V_1 such that

$$U_1(d_KD^{-1})\,V_1 = \begin{bmatrix} p^{k+1}A & 0 \\ 0 & p^kB \end{bmatrix}$$

where A and B are unimodular and diagonal. The lemma is obtained by dividing out d_K and taking inverses.

Remark. This lemma generalizes to $F = \mathbf{Q}$, but we do not need it here. The *norm group* of the lattice $\mathfrak{O}_K$ is defined to be the set

$$\mathfrak{g}\mathfrak{O}_K = Q(\mathfrak{O}_K) + 2\mathfrak{s}\mathfrak{O}_K.$$

We shall need the following.

LEMMA 3. *Let $F = \mathbf{Q}_2$. Suppose that $K \mid F$ is unramified. Then $\mathfrak{g}\mathfrak{O}_K = \mathfrak{O}_F$.*

Proof. Since $K \mid F$ is unramified, Q is a primitive form and so $\mathfrak{s}\mathfrak{O}_K = \mathfrak{O}_F$. Hence

$$\mathfrak{g}\mathfrak{O}_K = Q(\mathfrak{O}_K) + 2\mathfrak{O}_F.$$

Also, $e = 1$, and so we have

$$\overline{T_{K|F}(x)} = T_{\mathfrak{O}_K|\mathfrak{O}_F}(\bar{x}) \qquad \text{for all } x \in \mathfrak{O}_K.$$

Now suppose $a \in \mathfrak{O}_F$. Since $T_{\mathfrak{O}_K|\mathfrak{O}_F}$ is surjective, there is an $x \in \mathfrak{O}_K$ such

that $\bar{a} = T_{\bar{\mathfrak{O}}_K|\bar{\mathfrak{O}}_F}(\bar{x})$. Moreover $\bar{\mathfrak{O}}_K$ is a perfect field of characteristic two, and so there is a $z \in \mathfrak{O}_K$ such that $\bar{z}^2 = \bar{x}$. Hence

$$a \equiv Q(z) \pmod 2$$

and therefore $a \in \mathfrak{g}\mathfrak{O}_K$.

3. Proof of the Theorem

As before, let $V = K \otimes_{\mathbf{Q}} \mathbf{Q}_p$. It will be sufficient to prove that $\mathrm{cls}_{\mathfrak{p}}(\mathfrak{O}_K)_{\mathfrak{p}} = \mathrm{cls}_{\mathfrak{p}}(\mathfrak{O}_{K'})_{\mathfrak{p}}$ for all primes p if and only if condition (i) and (ii) of the theorem are satisfied. We first prove the necessity. If $\mathrm{gen}\,\mathfrak{O}_K = \mathrm{gen}\,\mathfrak{O}_{K'}$ then we clearly must have (i), and so $e(p) = e'(p) = 1$ for all primes p which do not divide d_K. Therefore assume p divides d_K. Then we have an isometry

$$(\mathfrak{O}_K)_{\mathfrak{p}} \cong \begin{bmatrix} M & 0 \\ & \\ 0 & pN \end{bmatrix},$$

where M and N are unimodular and diagonal. Let $\mathfrak{P}^{\delta}$ be the different, then, by normality, $p^{gf\delta}$ is the largest power of p which divides d_K, and so we have

$$\dim N = n - (n/e).$$

Hence the Jordan Splitting of $(\mathfrak{O}_K)_{\mathfrak{p}}$ is completely determined by the numbers $e(p)$. This proves the necessity.

Now assume conditions (i) and (ii). We must consider several cases.

Case 1. Suppose p is odd and does not divide d_K. Then each K_i is unramified and so each $\mathfrak{O}_{K_i}$ is unimodular. Therefore we obtain a splitting

$$(\mathfrak{O}_K)_{\mathfrak{p}} \cong \langle 1\rangle \perp \cdots \perp \langle 1\rangle \perp \langle d_K\rangle.$$

And so [2, 92:1a] $\mathrm{cls}_{\mathfrak{p}}(\mathfrak{O}_K)_{\mathfrak{p}} = \mathrm{cls}_{\mathfrak{p}}(\mathfrak{O}_{K'})_{\mathfrak{p}}$.

Case 2. Let $p = 2$. Then by hypothesis p does not divide d_K, and so again the $\mathfrak{O}_{K_i}$ are unimodular.

By lemma 3, we have $\mathfrak{g}(\mathfrak{O}_K)_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{p}}$, hence [2, 93:16] $\mathrm{cls}_{\mathfrak{p}}(\mathfrak{O}_K)_{\mathfrak{p}} = \mathrm{cls}_{\mathfrak{p}}(\mathfrak{O}_{K'})_{\mathfrak{p}}$.

Case 3. Suppose that p divides d_K.

We can assume that

$$A = \mathrm{diag}(1,\ldots, 1, a)$$

and

$$B = \mathrm{diag}(b, 1,\ldots, 1).$$

Therefore

$$(\mathfrak{O}_K)_p \cong \operatorname{diag}(1,\ldots, 1, a, bp, p,\ldots, p)$$

Let $J \cong \operatorname{diag}(a, bp)$, then a short computation shows that $S_p(\mathbf{Q}_p J) = S_p(\mathbf{Q}_p J')$. Since both J and J' are $\mathfrak{O}_p$-maximal, we have $\operatorname{cls}_p J = \operatorname{cls}_p J'$ and so $\operatorname{cls}_p(\mathfrak{O}_K)_p = \operatorname{cls}_p(\mathfrak{O}_{K'})_p$.

This completes the proof of the theorem.

Remark 1. The theorem of Taussky, quoted in Section 1, may be obtained by studying the algebra $K \otimes_{\mathbf{Q}} \mathbf{R}$, where $\mathbf{R}$ is the real field.

Remark 2. It is almost certain that the hypotheses of the theorem can be relaxed. The normality may not be essential, and the condition that the discriminants be odd was imposed because an investigation of the case when 2 ramifies is not yet complete.

References

1. H. B. Mann and K. Yamamoto, On canonical bases of ideals, *J. Combinatorial Theory* **2** (1967), 71–76.
2. O. T. O'Meara, "Introduction to Quadratic Forms," p. 117, Springer-Verlag, Berlin, 1963.
3. O. Taussky, The discriminant matrix of a number field, *J. London Math. Soc.* **43** (1968), 152–154.
4. O. Taussky, Ideal matrices. II, *Math. Ann.* **150** (1963), 218–225.
5. O. Taussky, On the similarity transformation between an integral matrix with irreducible characteristic polynomial and its transpose, *Math. Ann.* **166** (1966), 60–63.